シングルサインオン・システムの高信頼性のための設計方法について

第４事業部
セキュリティソリューション部
ソリューションチーム
ITスペシャリスト

中谷　辰五郎

Tatsugoro　Nakatani
tatsugoro-nakatani@exa-corp.co.jp

企業内外を問わずウェブアプリケーションの利用が一般的になるに伴い、その高度なセキュリティ対策の実現に必要なシングルサインオンシステムが注目されるようになった。また、法環境整備に伴う内部統制実現のためのIT全般統制システム実現の手段として、シングルサインオンシステムの重要性が認識され出している。その一方で、すべてのウェブアプリケーションの玄関となるシングルサインオンシステムに要求される、高い信頼性を確保するための一般的な設計方法はいまだ確立されていないという問題がある。

本稿では、この問題解決のためのアプローチ事例として、筆者の経験に基づく、可用性に重点を置いたシングルサインシステムの設計方法を紹介する。さらに、代表的なアーキテクチャを持つ２つの製品を取り上げ、紹介した設計方法に基づく試設計を行い、その結果の妥当性を検証し、考察した。

1. はじめに

近年、インターネット上で提供されている、情報検索サイト、各企業のホームページ、ネットショッピング、さらにはデイトレードやインターネットバンキングなどの多種多様なサービスが、ウェブアプリケーションで構築されている。また、企業内においても、情報共有や様々な業務処理のためにウェブアプリケーションが活発に利用されている。これに伴い、ウェブアプリケーションシステムに保管された個人情報や営業秘密の漏えいなどの情報セキュリティ事故が増加の一途をたどっている。この解決策として、ウェブアプリケーションに対する利用者の強固な認証やアクセス制限などを行うシングルサインオンシステムが注目されている。

また、IT化・ネットワーク化に伴う社会環境変化に対応するため、情報セキュリティやコンプライアンス視点から、個人情報保護法[1]をはじめ、金融商品取引法[2]や会社法[3]などの法環境整備が進んでいる。これら法律が共通して要請しているのは、企業の内部統制を実現するマネジメントシステムの構築であり、内部統制システムのインフラとなるIT全般統制の重要性を指摘している。適正なユーザが適切な業務(アプリケーションや情報など)を利用することを保証するシングルサインオンシステムは、このIT全般統制の主要なコンポーネントとしても認識されている。

シングルサインオンシステムは、最終的には企業内外の情報システムへのアクセスすべてにかかわるため、重要な基幹システムとして位置付けるべきものである。シングルサインオンシステムが停止すると、あらゆる業務に影響を及ぼし、ひいては事業の継続性確保が危うくなることも予想される。その一方で、このような高信頼性要求に応えるシングルサインシステム全般に対する設計法は、一般的に確立されているとは言いがたい状況にある。また、製品として提供されるシングルサインオンシステムごとにアーキテクチャが異なるため、これが設計に与える影響についても十分に把握されていないという問題がある。

本稿では、シングルサインオンシステムの設計にかかわる諸問題を解決するための一つのアプローチとして、可用性の確保に重点を置いた設計方法を紹介する。さらに、代表的な２つのアーキテクチャを持つ製品に対する可用性の設計例を示し、これを検証することにより、製品アーキテクチャの違いによる設計への影響について考察する。まず２章で、シングルサインオンシステムの概要について述べる。次に３章で、この分野で設計・構築に携わってきた筆者の経験事例に基づくシングルサインオンシステムの設計方法を紹介する。４章で、３章の方法に基づき、代表的なアーキテクチャを持つ２つの製品に対する設計例を示し、５章で設計方法の有効性とアーキテクチャごとの考慮点について考察する。

2. シングルサインオンシステムの概要

2.1. アーキテクチャ

シングルサインオンシステムのアーキテクチャは、リバースプロキシ型とエージェント型の２種類[4]に分けられる。リバースプロキシ型は、ウェブアプリケーションへのアクセスすべてを一台のシングルサインオン用のサーバが管理する方式であり、ウェブアプリケーションへのアクセスはシングルサインオン用サーバを常時経由する形となる。一方、エージェント型は、各ウェブアプリケーションサーバにエージェントと呼ばれるコンポーネントを導入する方式で、ウェブアプリケーションへのアクセスは、認証や認可時だけエージェントが介在する形態となる。

リバースプロキシ型に分類される製品として、IBM Tivoli Access Manager（以降TAMと称す）があり、エージェント型に分類される製品としてRSA Clear Trust（以降CTと称す）がある。

2.2. 主な機能

シングルサインオン・システムの主な機能には、認証、認可(アクセス制御)、ユーザやグループ(アクセス制御設定含む)管理がある。

① 認証は、IDとパスワードや電子証明書を利用して、あらかじめ登録してある情報と照合しユーザを特定する機能である。

② 認可は、あらかじめ設定しておいたアクセス制御情報に基づき、アクセス要求してきたユーザに対して、アクセスを認可・拒否する機能である。

③ ユーザ・グループ管理は、認証や認可で必要となるユーザ情報やアクセス制御情報を登録・管理するための機能である。グループは、アクセス制御をユーザ単位ではなく、まとまった単位で管理するための機能である。

表１に、上記の機能一覧を示す。なお、ここではユーザのパスワード変更は、パスワードは認証のために必要な情報であることから認証機能に含めた。

表１　シングルサインオンシステムの主な機能と操作

No.	機能		データ操作	ユーザが利用(*)
1	認証	認証	参照	○
2		パスワード変更	更新	○
3	認可	許可	参照	○
4	ユーザ・グループ管理	ユーザ登録	追加・更新・削除	—
5		グループ登録	追加・更新・削除	—
6		アクセス情報登録	追加・更新・削除	—

(*)「ユーザが利用」:エンドユーザWebサーバアクセス時に利用する機能
凡例:　○:　利用する、ー:利用しない

シングルサインオンシステムが停止すると、ウェブアプリケーションにアクセスできず、結果的に業務処理が止まることになる。シングルサインオンシステムの主な機能のうち、その機能が停止したとき、業務停止に直結するものは、ユーザがログイン時に使用する認証とパスワード変更機能、およびウェブアプリケーションへアクセスするときの認可機能である。そこで本稿では、これらの機能に焦点をあて、論じていくことにする。

2.3.　TAMの構成コンポーネントと認証、認可処理

2.3.1.　コンポーネント構成

TAMは、WebSEALサーバ､ポリシサーバ､およびLDAPサーバの３つのコンポーネントから構成される[5)]。

- WebSEALサーバは、認証や認可を実施するコンポーネントである。認証情報や認可情報を取得するため、ポリシサーバやLDAPサーバと通信する。
- ポリシサーバは、ユーザ・グループ登録やアクセス制御情報の登録を行うためのコンポーネントであり､ユーザ・グループ情報を格納するため、LDAPサーバと通信する。またアクセス制御情報は、自身に保管する。
- LDAPサーバはユーザ・グループ情報を格納するためのデータストアである。

図１にTAMのコンポーネント構成を示す。

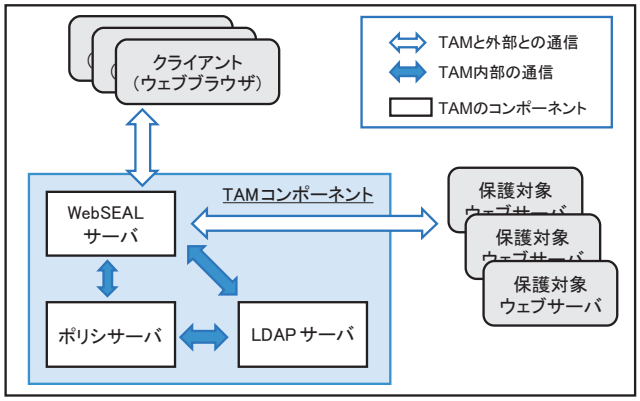


図１　TAMのコンポーネント構成

2.3.2.　認証の仕組み

TAMの認証処理概要を図２に示す。認証の流れは以下のとおりである。

① クライアント(ウェブブラウザ)からの画面表示要求をWebSEALサーバが受ける。
② WebSEALサーバは、ユーザ認証が終わっていないためログイン画面をクライアントに送信する。
③ ユーザがIDとパスワードをログイン画面に入力し送信する。
④ WebSEALサーバは認証のためにLDAPサーバへユーザIDとパスワードの照合を要求する。
⑤ LDAPサーバは照合結果をWebSEALサーバに戻す。
⑥ WebSEALサーバは、認証が成功した場合、ユーザが①で要求した画面へのリダイレクト、および今後の認証処理で利用するCookieをブラウザに戻す。
⑦ ブラウザは､リダイレクトにより目的の保護対象ウェブサーバにアクセスする。
⑧ 保護対象ウェブサーバは要求された画面をブラウザに戻す。

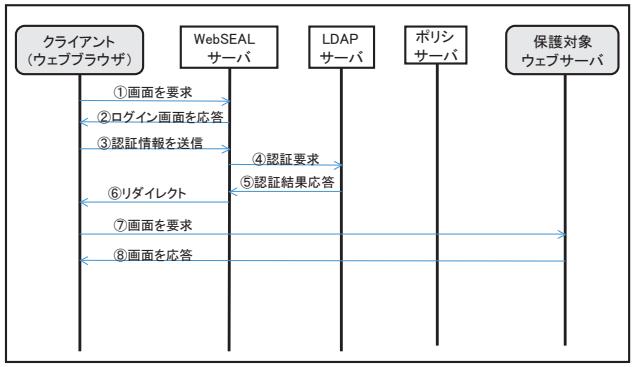


図２　TAMの認証処理

2.3.3.　パスワード変更の仕組み

TAMのパスワード変更処理概要を図３に示す。パスワー

ド変更の流れは以下のとおりである。

① クライアントはWebSEALサーバにパスワード変更画面を要求する。
② WebSEALサーバはブラウザにパスワード変更画面を戻す。
③ ユーザは変更するパスワードを入力し、パスワード変更をWebSEALサーバに要求する。
④ WebSEALサーバはLDAPサーバに対して入力されたパスワードに置き換えるようにLDAPサーバに要求する。
⑤ LDAPサーバはパスワード変更結果をWebSEALサーバに戻す。
⑥ WebSEALサーバはパスワード変更結果をブラウザに戻す。

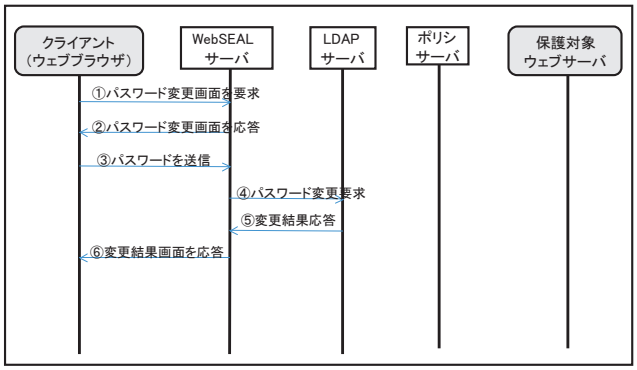


図３　TAMのパスワード変更処理

2.3.4. 認可の仕組み

① WebSEALサーバは、認証時にクライアントに送ったCookieを元に、アクセスしてきているユーザを識別し、WebSEALサーバ内に保持するアクセス制御情報と照合して、当該アクセスの可否を決める。（注：　WebSEALサーバは、ポリシサーバの保持するアクセス制御情報のコピーを保持している）
② アクセス可の場合、WebSEALサーバは、ブラウザと保護対象Webサーバ間での通信のためのリバースプロキシーとして作動する。アクセス不可の場合、WebSEALサーバは、ブラウザにアクセス不可を返し、通信を終了する。

2.4. CTの構成コンポーネントと認証

2.4.1. コンポーネント構成

CTは、WebAgent、ClearTrustサーバ、およびLDAPサーバの３つのコンポーネントから構成される[6)]。

- WebAgentは、保護対象ウェブサーバのモジュール内部にライブラリとして組み込まれ、認証、認可のフロントエンド処理を行う。WebAgentは、認証および認可のためにClearTrustサーバと通信する。
- ClearTrustサーバは、認証、認可処理そのものを行う。またClearTrustサーバは、ユーザ・グループの登録およびアクセス制御情報の登録を処理する。ClearTrustサーバは、認証、認可や登録処理のためにLDAPサーバと通信する。
- LDAPサーバはユーザ・グループ情報やアクセス制御情報を保管するためのデータストアである。

CTのコンポーネント構成を図４に示す。

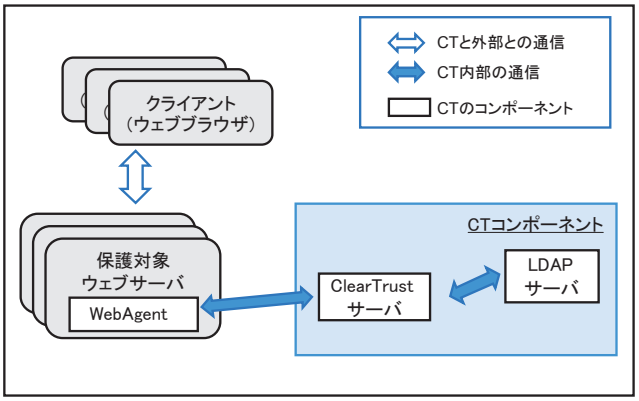


図４　CTのコンポーネント構成

2.4.2. 認証の仕組み

CTの認証処理概要を図５に示す。認証の流れは以下のとおりである。

① クライアント(ウェブブラウザ)からの画面表示要求を保護対象ウェブサーバ内のWebAgentが受ける。
② ユーザ認証が終わっていないためログイン画面をクライアントに送信する。
③ ユーザがIDとパスワードをログイン画面に入力し送信する。
④ WebAgentは認証のためにClearTrustサーバへ認証

処理を要求する。

⑤ ClearTrustサーバは、認証のためにLDAPサーバに認証を要求する。

⑥ LDAPサーバは照合結果をClearTrustサーバに戻す。

⑦ ClearTrustサーバは、認証結果をWebAgentに戻す。

⑧ WebAgentは認証が成功した場合、ユーザが①で要求した画面へのリダイレクトおよび今後の認証処理で利用するCookieをブラウザに戻す。

⑨ ブラウザは、リダイレクトにより目的の保護対象ウェブサーバにアクセスする。

⑩ 保護対象ウェブサーバは要求された画面をブラウザに戻す。

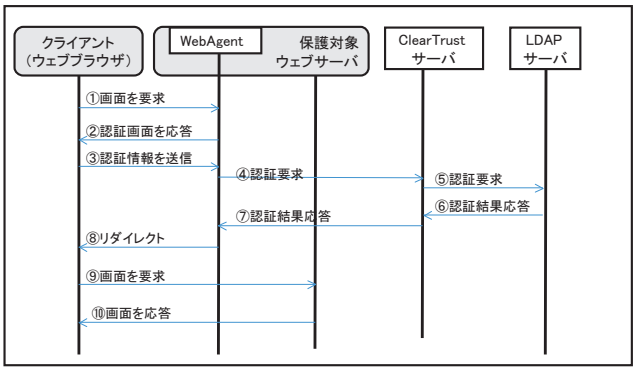


図５　CTの認証処理

2.4.3. パスワード変更の仕組み

CTのパスワード変更処理概要を図６に示す。パスワード変更の流れは以下のとおりである。

① クライアントは保護対象ウェブサーバにパスワード変更画面を要求する。

② 保護対象ウェブサーバはブラウザにパスワード変更画面を戻す。

③ ユーザは変更するパスワードを入力し、パスワード変更を保護対象ウェブサーバに要求する。

④ 保護対象ウェブサーバはパスワード変更をClearTrustサーバに要求する。

⑤ ClearTrustサーバはLDAPサーバに対して入力されたパスワードに置き換えるようにLDAPサーバに要求する。

⑥ LDAPサーバはパスワード変更結果をClearTrustサーバに戻す。

⑦ ClearTrustサーバはパスワード変更結果を保護対象ウェブサーバに戻す。

⑧ 保護対象ウェブサーバはパスワード変更結果をブラウザに戻す。

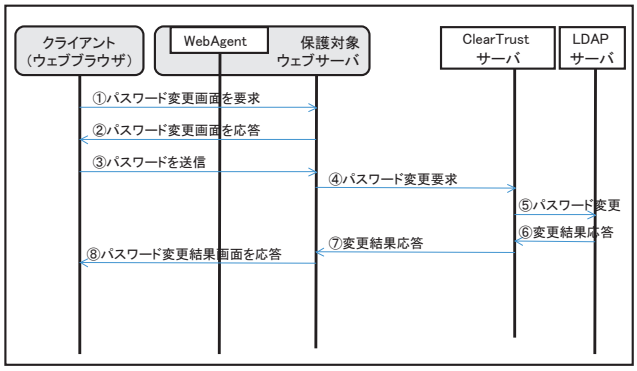


図６　CTのパスワード変更処理

2.4.4. 認可の仕組み

① WebAgentは、認証時にクライアントに送ったCookieを元に、アクセスしてきているユーザを識別し、ClearTrustサーバに認可を要求する。ClearTrustサーバはアクセス制御情報と照合して、当該アクセスの可否を決め、WebAgentに応答する。

② アクセス可の場合、WebAgentは、保護対象ウェブサーバに対してブラウザからの要求を引き渡す。アクセス不可の場合、WebAgentは、保護対象ウェブサーバにアクセス不可のエラーを返す。

3. シングルサインオンシステムの設計方法

シングルサインオンシステムの設計は、機能要件と非機能要件に対応する設計に分けられる。その高信頼性に影響を与える設計項目は、一般に非機能要件側に分類される。非機能要件側に分類される設計項目としては、大きく分けて、可用性設計、性能設計、運用設計、セキュリティ設計、および拡張性設計などがある。

非機能要件の設計は、通常、性能や冗長化などのハードウエア構成（システム構成）に大きく依存する。システム構成に影響する主な設計項目は、可用性設計、性能設計、および運用設計の３つである。

本稿では、「シングルサインオンシステムの設計の基本は、高信頼性を実現するためのシステム構成の設計である」という考え方に基づき、可用性、性能、運用の３つの設計項

目を中心にした設計フローを提案する。これを図７に示す。

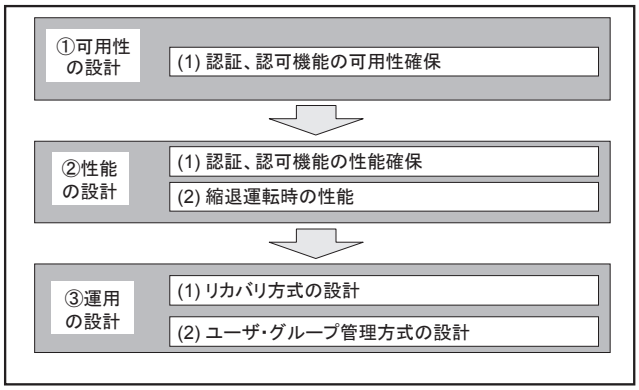


図７　可用性、性能、運用要件の設計フロー

一般にシステム構築においてすべての可用性、性能、運用要件を最適化して実装することはコストとの関係で難しい場合が多く、要件に順位付けを行い、その順位の高い要件から設計する。

シングルサインオンシステムの場合、性能面は多少遅くてもある程度許容される場合が多いが、サービス停止は許容されないため、可用性の設計に重点を置き、①可用性の設計、②性能の設計、③運用の設計の順で行う。③運用の設計を最後に行っているのは、①、②で設計したシステム構成に対する運用が適切かを確認するためである。

3.1. 可用性の設計

(1) 認証、認可機能の可用性設計

認証、認可機能に対しては、基本的に可用性確保の仕組みが製品で提供されている。したがって製品仕様に基づき、認証、認可の可用性を確保するためのシステム構成を設計する。

具体的には、認証、認可に影響を与えるコンポーネントの可用性を確保するための冗長構成を設計する。

認証および認可機能で、ログイン時の認証、ウェブアプリケーションへのアクセス時の認可処理は、LDAPサーバに対する参照処理である。またパスワード変更処理は、LDAPサーバに対する更新処理である。したがって、認証、認可の処理機能の可用性確保、およびLDAPサーバに対する参照、更新処理機能の可用性確保を考慮する。ここでLDAPサーバの冗長構成は、その方式の違いから実現できる可用性要件が異なるため、システム構成を決定する要因として重要である。

3.2. 性能設計

(1) 認証、認可機能の性能確保

シングルサインオンシステムでは、ユーザ数が多いほど、認証や認可処理の負荷が高くなる。この負荷が高くなると、業務システムにアクセスしようとしても、ログオン画面やアクセスしたいWebの画面が返ってくるまでに、ユーザが許容できない時間を要することになる。

したがって、認証と認可という点で性能設計を行う際、下記の事項を検討し設計する。

(a) 認証(ログイン)

単位時間(ピーク時)にログインするユーザ数。業務開始時や昼休憩後の時間帯を想定する。

(b) 認証(パスワード変更)

単位時間(ピーク時)にパスワード変更するユーザ数。パスワードポリシーに、パスワード有効期間を設けた場合に、システム移行時に登録するユーザのパスワード有効期限が同じになるため、パスワード有効期限満了日の業務開始時にパスワード変更が集中することを想定する。

(c) 認可

単位時間(ピーク時)にアクセスするページ数。

リバースプロキシ型の場合は、認可処理件数以外に、保護対象サーバへユーザからのリクエストを送り、その結果をユーザへ返す処理も行うため、ネットワークの通信量の設計が必要である。通信量を導出するためには、１ページあたりの平均コンテンツ数(１ページに表示するGIF,JPEGなどのイメージの数など)と、１コンテンツあたりの平均サイズ(kB)を調査する。

エージェント型の場合は、ユーザからアクセスする通信量は、既存の保護対象ウェブサーバが処理する通信量と変わらない。

(2) 縮退運転時の性能

システム障害が発生した場合の縮退運転時の性能を設計しておく必要がある。処理速度自体は縮退運転のため低下するのは明らかだが、その他に必要な項目としてリソース(プロセスメモリ)の確保がある。

一般的にシングルサインオンシステムは、セッション情報をサーバ内部(メモリ上)に格納し認可処理を高速化している。縮退運転時は、このセッション情報が増加するため通常以上のメモリを使用することになる。

このため、縮退運転時においてもリソースが確保できるように設計する必要がある。

3.3. 運用設計

(1) リカバリ方式の設計

シングルサインオンシステムの高信頼性を実現するため、認証、認可の視点で運用設計を論じる場合、障害時に、認証、認可の機能を復旧するためのリカバリ方式の設計が重要である。

リカバリ方式の設計において重要な考慮事項は、復旧時間であることはいうまでもないが、それ以外にリカバリ手順の容易さも大切である。分散システムの場合、運用コストの削減のため、各システムに専門の運用者を配置できることは少なく、複数のサーバの管理を同じ運用者が担うことが多い。このようなケースも想定して、できるだけ容易にリカバリが行えることも重要になる。

また、リカバリ方式を設計するときには、実際に運用が可能なことを確認しておくことを忘れてはならない。

(2) ユーザ・グループ管理方式の設計

障害時に、認証、認可の機能を復旧する上では、ユーザ・グループ情報の復旧に関する考慮が必要である。

ユーザ・グループ情報の管理を製品付随のGUIで行う場合は、システム構成が影響を与えることはないが、別システムからユーザ・グループなどのデータを一括取得し登録するようなバッチ処理が存在する場合、システム構成を考慮した運用設計を行う必要がある。

例えば、ユーザ・グループ情報を格納するLDAPサーバがHA方式の場合、LDAPサーバ障害時は、HA機能によりスタンバイ機へ自動的に切替えるため、バッチ処理自体に障害対策機能(接続先LDAPサーバの切替処理)を組み込む必要はない。しかし、LDAPサーバがマルチ・マスタ方式の場合は、バッチ処理自身に障害対策機能を組み込む必要がある。

4. 冗長構成の設計例

4.1. 冗長構成の特徴

可用性と性能要件を満足するために、システムの冗長化方式を定める冗長構成の設計が最大のポイントとなる。まず、TAMとCTを対象に、各製品で提供している冗長構成の特徴について述べる。いずれの製品も可用性や性能向上のために、冗長構成を可能としている。製品の冗長構成の特徴を障害対策および負荷分散の機能面から表２に示す。

リバースプロキシ型であるTAMと、エージェント型であるCTでは、アーキテクチャの違いにより取り得る冗長構成の形態が異なる。また、シングルサインオンシステムでは認証・認可データの可用性確保が重要であるが、この冗長構成に関しても、CTでは共にLDAPサーバで管理しているが、TAMでは認証データはLDAPサーバ、認可データはポリシサーバで管理するという違いを考慮する必要がある。

ここでは、まず共通に利用されるLDAPサーバの冗長化方式について述べ、次にこれと連携して動作するTAMとCTの冗長構成の特徴について述べる。

表２　シングルサインオンシステムの冗長構成の特徴

No.	製品			特徴			
		コンポーネント		障害対策		負荷分散	
1	TAM	WebSEAL サーバ		負荷分散機により切替が可能	○	負荷分散機により要求の振分けが可能	○
2	TAM	ポリシサーバ		HA 機能により切替が可能	○	負荷分散機能は無い	×
3	TAM	LDAP サーバ	HA 方式	HA 機能により切替が可能	○	負荷分散機能は無い	×
4	TAM	LDAP サーバ	マスタ・スレーブ方式	障害対策機能は無い	×	WebSEAL サーバ、ポリシサーバにより要求の振分けが可能	○
5	TAM	LDAP サーバ	マルチ・マスタ方式	WebSEAL サーバ、ポリシーサーバにより切替が可能	○	WebSEAL サーバ、ポリシサーバにより要求の振分けが可能	○
6	CT	WebAgent		ウェブサーバの障害機切替方式に依存	–	ウェブサーバの負荷分散方式に依存	–
7	CT	ClearTrustサーバ		WebAgentによる障害サーバの切替が可能	○	WebAgentにより要求の振分けが可能	○
8	CT	LDAP サーバ	HA 方式	HA 機能により切替が可能	○	負荷分散機能は無い	×
9	CT	LDAP サーバ	マスタ・スレーブ方式	障害対策機能は無い	×	負荷分散機能は無い	×
10	CT	LDAP サーバ	マルチ・マスタ方式	障害対策機能は無い	×	負荷分散機能は無い	×

凡例:　○:機能がある。×:機能が無い。ー:他システムに依存。

4.1.1. LDAPの冗長化方式

LDAPサーバの冗長化方式として一般的な、HA方式、マスタ・スレーブ(レプリカ)方式、マルチ・マスタ(マスタ・マスタ)方式の３方式を取り上げる。

(1) HA方式

アクティブ､スタンバイの構成で､アクティブ側がLDAPサービスを提供する。アクティブ側で障害が発生した場合は、スタンバイ側に自動で切替わりLDAPサービスを継続する。常時稼動するLDAPサーバは１台のため負荷分散には利用できない。

(2) マスタ・スレーブ方式

参照および更新(追加・変更・削除)が可能なマスタと参照のみ可能なスレーブで構成する。LDAPのデータはマス

タ側で更新され、スレーブ側にレプリケーション(データの同期)を行う。

マスタ側で障害が発生した場合、スレーブ側で参照のみのサービスを継続する。また参照に関してはマスタおよびスレーブで提供できるため参照処理の負荷分散に利用できる。

(3) マルチ・マスタ方式

参照および更新が可能なマスタ複数台で構成される。LDAPのデータは各マスタで更新され、他のマスタにレプリケーション(データの同期)を行う。

あるマスタ側で障害が発生した場合、他のマスタで参照および更新のサービスを継続する。また参照および更新を複数のマスタで提供できるため、参照および更新処理の負荷分散に利用できる。

4.1.2. TAMの冗長構成の特徴

TAMの認証・認可を処理するWebSEALサーバは、負荷分散機による障害対策、負荷分散の機能を提供する。

ユーザ・グループ管理およびアクセス制御情報を保管するポリシサーバは、HA方式による障害対策の機能を提供する。

WebSEALサーバおよびポリシサーバは、マスタ・スレーブ方式またはマルチ・マスタ方式のLDAPサーバ構成に対応した障害対策、負荷分散の機能を提供する。なおマスタ・スレーブ方式の場合、LDAPサーバに対する更新の障害対策と負荷分散は行えない。

4.1.3. CTの冗長構成の特徴

CTの認証・認可の処理を要求するWebAgentは、WebAgentを組み込むウェブアプリケーションサーバの冗長構成に依存する。

CTの認証・認可を処理するClearTrustサーバは、WebAgent機能により障害対策および負荷分散の機能を提供する。

ClearTrustサーバは、マスタ・スレーブ方式またはマルチ・マスタ方式のLDAPサーバへの参照処理に対して障害対策の機能を提供するが、更新処理に対する障害対策機能は提供しない。またClearTrustサーバは、LDAPサーバに対して負荷分散機能を提供しない。

4.2. 冗長構成の設計例

本節では、TAM、CTそれぞれに対して行った冗長構成の設計例を示す。シングルサインオンシステムの冗長構成設計では、認証・認可を行う機能（例えばWebSEAL）と、認証・認可用のデータベース機能（例えばLDAP）との冗長構成の組合せパターンが存在する。それぞれの組合せパターンに対し、障害時の影響を検証しながら設計を進める必要があるが、この検証については次章で述べる。

ここでは、構築するマシンの数は、可用性を考慮した場合の最小構成となる４台構成とした。また、２重障害以上の障害ケースは複雑であり、一般の構築プロジェクトにおいても扱わないことが多いため割愛した。

4.2.1. TAMの冗長構成

TAMのWebSEALサーバは、一般的なウェブサーバと同様に負荷分散機による冗長構成をとる。

またポリシサーバは、アクセス制御データを保管するコンポーネントであることから、４台構成にする場合は、データに対するセキュリティ確保を考慮しLDAPサーバと同じデータ保管マシンに配置し、ユーザからのフロント処理を行うWebSEALサーバとは同居させない。

TAMの冗長構成を図８に示す。

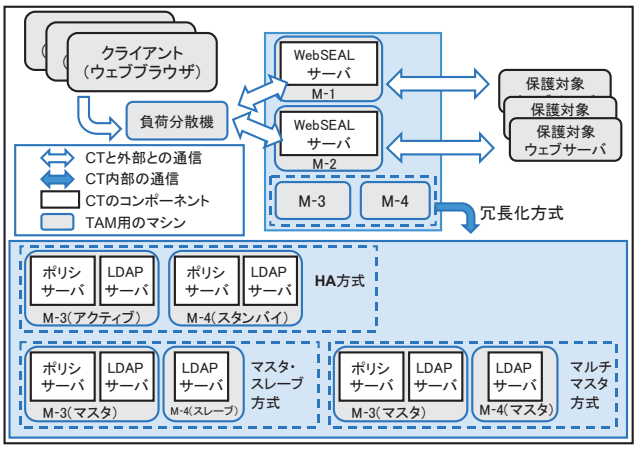


図８　TAMの冗長構成

M-1、M-2には、認証・認可機能の可用性を考慮し、WebSEALサーバをそれぞれ配置する。データ管理を司るLDAPサーバも可用性を考慮しM-3 、M-4 の２台に配置する。ここでLDAPサーバの冗長構成には、HA方式、マ

スタ・スレーブ方式およびマルチ・マスタ方式の３種類が考えられるが、それぞれの場合について図８に示してある。TAMのポリシサーバは、HA構成で冗長構成が可能であるが、それ以外の構成ではシングル構成となるため、HA方式の場合、M-3、M-4に配置し、マスタ・スレーブ方式およびマルチ・マスタ方式の場合、M-3(マスタ)に配置する。

WebSEALサーバ系とLDAPサーバ系を統合したシステム全体系の可用性を考慮する必要があるが、これについて考察する。

WebSEALサーバとLDAPサーバ間の通信は、WebSEALサーバ側に２台のLDAPサーバ情報を登録することで、WebSEALサーバが接続中のLDAPサーバに障害を検知したとき、自動でもう一台のLDAPサーバに切替える仕組みとする。

ポリシサーバもWebSEALサーバと同様にポリシサーバ側に２台のLDAPサーバ情報を登録することで、WebSEALサーバが接続中のLDAPサーバに障害を検知した場合、自動でもう一台のLDAPサーバに切替える仕組みとする。

4.2.2. CTの冗長構成

CTのWebAgentは、保護対象ウェブサーバにモジュール・ライブラリとして組み込まれるため、冗長構成は保護対象ウェブサーバの構成に依存する。保護対象ウェブサーバの冗長構成はシングルサインオンシステムの冗長構成に影響を与えないため、本稿では特に明示していない。

４台構成にする場合、ClearTrustサーバ２台、LDAPサーバ２台の構成とする。

CTの冗長構成を図９に示す。

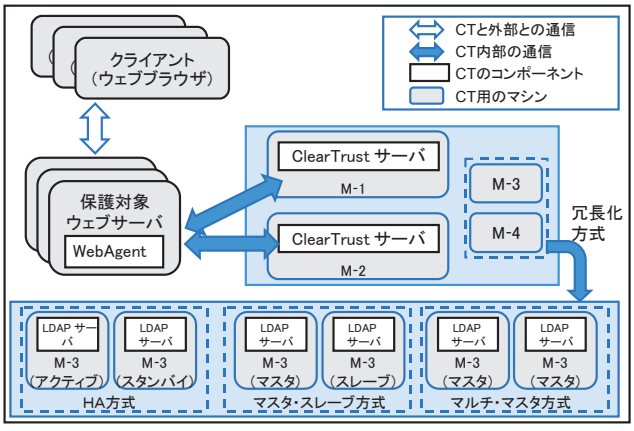


図９　CTの冗長構成

M-1、M-2には、認証・認可機能の可用性を考慮し、ClearTrustサーバをそれぞれ配置する。データ管理を司るLDAPサーバも可用性を考慮しM-3 、M-4 の２台に配置する。ここでLDAPサーバの冗長構成には、HA方式、マスタ・スレーブ方式およびマルチ・マスタ方式の３種類が考えられるが、それぞれの場合について図９に示してある。

WebAgent系とClearTrustサーバ系、およびClearTrustサーバ系とLDAPサーバ系を統合したシステム全体系の可用性を考慮する必要があるが、これについて考察する。

WebAgentとClearTrustサーバ間の通信は、WebAgentに２台のClearTrustサーバのマシン情報を登録することで、WebAgentがClearTrustサーバの障害を検知したとき、自動でもう一台のClearTrustサーバに切替える仕組みとする。

ClearTrustサーバとLDAPサーバ間は、ClearTrustサーバに、２台のLDAPサーバの接続情報を登録することで、ClearTrustサーバがLDAPサーバの障害を検知したとき、自動でもう一台のLDAPサーバに切替える仕組みとする。

5. 製品と構成の違いによるサービスの影響

前章で提示した設計例のそれぞれに対し、３章の設計方法で述べた３項目のうち優先順位の一番高い可用性確保に関して、システム構成の違い、製品の違いによるサービスへの影響を示す。

サービスへの影響の検証では、LDAPサーバの参照および更新処理の可用性確保で構成が異なるため、認証、認可機能のうち、ログイン時の認証処理およびパスワード変更処理を検証する。

5.1. 障害の種類

シングルサインオンシステムの障害の種類としては、大きくハードウエア障害、ソフトウエア障害、およびネットワーク障害に分類できる。障害の種類を表３に示す。

表３　シングルサインオンシステムの障害の種類

No	障害の種類	内容	備考
1	ハードウエア	マシン構成要素(CPU/メモリ/マザーボード/ディスク、ネットワークインターフェイス、電源など)の障害	
2	ソフトウエア	・OSの障害(OSパニックなど) ・シングルサインオン構成コンポーネントの障害	
3	ネットワーク	・ネットワークケーブルの断線 ・スイッチ、ルータなどのネットワーク機器の障害	

ハードウエア障害は、構成要素を二重化することで回避可能である。ネットワーク障害も同様にネットワーク機器の二重化で障害を回避することが可能である。

ここでは、シングルサインオン製品の冗長化機能の障害時の動作を考察することが目的であるため、ソフトウエア障害が発生した想定で動作を調査した。

5.2. TAMの障害時のサービスへの影響

5.2.1. 障害発生箇所と認証サービスへの影響

図２のTAMの認証処理において、ソフトウエア障害の発生ポイントとして、各ソフトウエアコンポーネントが動作する各サーバ上で、各々障害が生じた場合の動作と認証サービスへの影響を以下に示す。

(1) WebSEALサーバ障害時

(a) M-1が障害の場合のサーバ動作

図２の「①画面を要求」のとき、負荷分散機はM-1が障害であることを検知するので、M-2のWebSEALサーバにクライアントからの要求を送る。

(b) M-2が障害の場合のサーバ動作

M-2が障害の場合は、M-1が障害の場合とは逆に、負荷分散機が、M-1にクライアントからの要求を送信する。

(c) WebSEALサーバ障害時の認証サービスへの影響

上記(a)、(b)の動作により、WebSEALサーバ障害時の認証サービスは継続される。

(2) LDAPサーバ障害時

(a) M-3が障害の場合のサーバ動作 (HA方式)

図２の「④認証要求」のとき、M-3で障害が発生しているため、HAの機能によりLDAPサーバはM-4に切替わっている。なおM-4はスタンバイであるため、M-4が障害のケースは考慮しない。

(b) M-3が障害の場合のサーバ動作(マスタ・スレーブ方式)

図２の「④認証要求」のとき、M-3で障害が発生しているため、WebSEALサーバがM-4のLDAPサーバに対して照合を要求する。

(c) M-4が障害の場合のサーバ動作(マスタ・スレーブ方式)

M-4が障害の場合は、WebSEALサーバがM-3のLDAPサーバに対して照合を要求する。

(d) M-3が障害の場合のサーバ動作(マルチ・マスタ方式)

図２の「④認証要求」のとき、M-3で障害が発生しているため、WebSEALサーバがM-4のLDAPサーバに対して照合を要求する。

(e) M-4が障害の場合のサーバ動作(マルチ・マスタ方式)

M-4が障害の場合は、WebSEALサーバがM-3のLDAPサーバに対して照合を要求する。

(f) LDAPサーバマシン障害時の認証サービスへの影響

上記(a)から(e)の動作から、HA方式、マスタ・スレーブ方式、およびマルチ・マスタ方式のいずれの場合も、認証サービスは継続される。

5.2.2. 障害発生箇所とパスワード変更サービスへの影響

図３のTAMのパスワード更新処理で、前節同様にソフトウエア障害の発生ポイントとして、各ソフトウエアコンポーネントが動作する各サーバ上で、各々障害が生じた場合のサーバ動作とパスワード変更サービスへの影響を以下に示す。

(1) WebSEALサーバ障害時

(a) M-1が障害の場合のサーバ動作

図３の「①パスワード変更画面を要求」のとき、負荷分散機はM-1が障害であることを検知しているので、M-2のWebSEALサーバにクライアントからの要求を送信する。

(b) M-2が障害の場合のサーバ動作

M-2が障害の場合は、M-1が障害のときとは逆に、負荷分散機が、M-1にクライアントからの要求を送信する。

(c) WebSEALサーバ障害時のパスワード変更サービスへの影響

上記(a)、(b)のサーバ動作により、パスワード変更サービスは継続される。

(2) LDAPサーバ障害時

(a) M-3が障害の場合のサーバ動作 (HA方式)

図３の「④パスワード変更要求」のとき、M-3で障害が発生しているため、HAの機能によりLDAPサーバはM-4に切替わっている。なおM-4はスタンバイであるため、M-4が障害のケースは考慮しない。

(b) M-3が障害の場合のサーバ動作(マスタ・スレーブ方式)

図３の「④パスワード変更要求」のとき、M-3で障害が発生しているため、パスワード更新処理が可能なLDAPサーバが存在しない。

(c) M-4が障害の場合のサーバ動作(マスタ・スレーブ方式)

図３の「④パスワード変更要求」のとき、M-4で障害が

発生しているが、WebSEALサーバはM-3のLDAPサーバにしか要求しない。

(d) M-3が障害の場合のサーバ動作(マルチ・マスタ方式)

図３の「④パスワード変更要求」のとき、M-3で障害が発生しているため、WebSEALサーバはM-4のLDAPサーバに要求する。

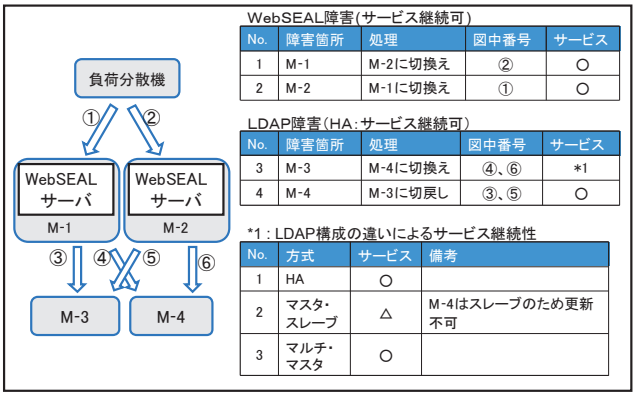
(e) M-4が障害の場合のサーバ動作(マルチ・マスタ方式)

図３の「④パスワード変更要求」のときM-4で障害が発生しているため、WebSEALサーバはM-3のLDAPサーバに要求する。

(f) LDAPサーバ障害時のパスワード変更サービスへの影響

- HA方式の場合、上記(a)のサーバ動作により、パスワード変更サービスは継続される。
- マスタ・スレーブ方式の場合、上記(b)、(c)のサーバ動作により、マスタ側(M-3)が障害の場合に、パスワードサービスは継続できない。
- マルチ・マスタ方式の場合、上記(d)、(e)のサーバ動作により、パスワード変更サービス継続される。

以上の結果を図10に示す。



WebSEAL障害(サービス継続可)

No.	障害箇所	処理	図中番号	サービス
1	M-1	M-2に切換え	②	○
2	M-2	M-1に切換え	①	○

LDAP障害(HA:サービス継続可)

No.	障害箇所	処理	図中番号	サービス
3	M-3	M-4に切換え	④、⑥	*1
4	M-4	M-3に切戻し	③、⑤	○

*1 : LDAP構成の違いによるサービス継続性

No.	方式	サービス	備考
1	HA	○	
2	マスタ・スレーブ	△	M-4はスレーブのため更新不可
3	マルチ・マスタ	○	

図10　障害時の動作(TAM)

5.3. CTの障害時のサービスへの影響

次にCTにおける図５の認証処理、および図６のパスワード変更処理において、ソフトウエア障害の発生ポイントとして、各ソフトウエアコンポーネントが動作する各サーバ上で障害が生じた場合のサービスへの影響を、TAMの場合と同様に考察すると以下のようになる。

5.3.1. 障害発生箇所と認証サービスへの影響

(1) ClearTrustサーバマシン障害時

M-1およびM-2が障害の場合でも、WebAgentにより正常に稼動しているClearTrustサーバが選択されるため、認証サービスは継続される。

(2) LDAPサーバ障害時

M-3およびM-4が障害の場合、HA方式ではHAがLDAPサーバの障害を検知し切替えるため、マスタ・スレーブ方式およびマルチ・マスタ方式ではClearTrustサーバがLDAPサーバの障害を検知し切替わるため、認証サービスは継続される。

5.3.2. 障害発生箇所とパスワード変更サービスへの影響

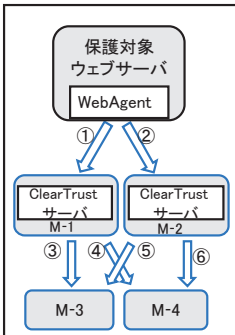
(1) ClearTrustサーバ障害時

M-1およびM-2が障害の場合でも、WebAgentにより正常稼動しているClearTrustサーバが選択されるため、パスワード変更サービスは継続される。

(2) LDAPサーバ障害時

- HA方式の場合、HAの切替/切戻し機能により、パスワード変更サービスは継続される。
- マスタ・スレーブ方式およびマルチ・マスタ方式の場合、M-3(マスタ)障害時は、製品仕様により更新可能なLDAPサーバを切替えることができないため、パスワード変更サービスは継続できない。

以上の結果を図11に示す。



ClearTrust障害(サービス継続可)

No.	障害箇所	処理	図中番号	サービス
1	M-1	M-2に切換え	②	○
2	M-2	M-1に切換え	①	○

LDAP障害(HA:サービス継続可)

No.	障害箇所	処理	図中番号	サービス
3	M-3	M-4に切換え	④、⑥	*1
4	M-4	M-3に切戻し	③、⑤	○

*1 : LDAP構成の違いによるサービス継続性

No.	方式	サービス	備考
1	HA	○	
2	マスタ・スレーブ	△	M-4はスレーブのため更新不可
3	マルチ・マスタ	△	CTの仕様上更新機能の切換え不可のため、更新不可

図11　障害時の動作(CT)

5.4. 製品アーキテクチャによる差異の考察

5.2節、5.3節で考察した、TAM、CTそれぞれに対する障害発生時のサービスに対する影響をまとめて表４に示す。

表４　LDAPの冗長構成の方式と障害時のサービス継続性

No	対象機能	TAM			CT		
		HA	マスタ・スレーブ	マルチ・マスタ	HA	マスタ・スレーブ	マルチ・マスタ
1	認証（参照処理）	○	○	○	○	○	○
2	パスワード変更（更新処理）	○	△	○	○	△	△

凡例：
○：障害時でもサービスが継続できる
△：障害時にサービスが継続出来ない場合がある

同表から、認証機能、特に更新処理を伴うパスワード変更に関して、TAMとCTいずれの場合にもサービスを継続できない場合があり、これがLDAPサーバの構成に依存していることが分かる。つまり、シングルサインオンシステムの高信頼性に影響を与える設計上のポイントは、LDAPサーバの構成であるとも言える。

また、LDAPサーバがマルチ・マスタ構成の場合、パスワード変更のサービス継続性にTAMとCTでは違いがあり、製品アーキテクチャによる可用性の実現レベルにも配慮が必要なことが分かる。

このことから、シングルサインオンシステムの設計を進める上で、下記の２点が大切である。

① 製品アーキテクチャによる冗長化の仕組みと、実現可能な可用性レベルの理解、特にLDAPサーバ冗長化の仕組みとの対応関係の理解
② 認証機能、特にパスワード変更に対する更新処理の要件レベルの早期の明確化

6. おわりに

本稿では、シングルサインオンシステムの設計方法確立に向けたアプローチとして、企業の認証基盤として要求される高信頼性確保に重点を置いた、実践的な方法を提案した。また、アーキテクチャの異なる２つの製品（TAMとCT）に対し試設計を行い、具体的な事例として示すと同時に、その結果を考察することにより、次に示す、いくつかの知見を得た。

① 製品アーキテクチャ、特に認証、認可、パスワード変更機能に対する冗長構成方式の理解が重要である。
② 冗長構成設計の中で、認証・認可データの格納庫となるLDAPサーバの冗長構成設計がシステム全体のサービス継続性（高信頼性）に大きな影響を与える。
③ 更新処理を伴うパスワード変更機能に対する可用性要求（サービス継続性の実現レベル）が、システムの冗長構成を決める重要な設計要件になる。

シングルサインオンシステムは、企業の基幹システムとして益々利用が拡大していくと考えられる。また、シングルサインオンシステム製品にも、新たな機能追加やアーキテクチャの変革が生じている。本稿で提案した設計方法や得られた知見は、シングルサインオンの基本機能である認証・認可・パスワード変更という普遍的な機能と、高信頼性確保という普遍的な要求に着目したものであり、このような環境・技術変化に対しても有効な手段であると考えている。

そうは言っても、新しい製品アーキテクチャを吸収する形で、設計方法を改善・改良していく必要があることは言うまでもない。今後、本稿で示した設計方法を、様々なシングルサインオンシステム構築プロジェクトに適用し、シングルサインオンシステムの高信頼性確保に繋げると共に、設計方法をさらにブラシュアップしていく所存である。

参考文献

1) 個人情報保護法
http://www5.cao.go.jp/seikatsu/kojin/index_sub001.html、個人情報の保護に関する法律
2) 金融商品取引法
http://www.fsa.go.jp/policy/kinyusyohin/pamphlet.pdf
3) 会社法の概要
http://www.moj.go.jp/HOUAN/houan33.html、会社法の条文はこちら(PDF)
4) 「シングルサインオンとは」
http://www.keyman.or.jp/search/security2/30001292_1.html?vos=nkeyadww07030903
5) IBM Tivoli Access Manager　バージョン5.1 Base管理者ガイド、P9-P10、WebSEAL管理者ガイド、P6-P7
6) RSA Clear Trust バージョン 5.5.3 Server Installation and Configuration Guide、P15.
